AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Kimberly Vagos Blackwood, being duly sworn, depose and say:

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for over thirteen years. I am currently assigned to the FBI's Lowell, Massachusetts Resident Agency. As a member of this Resident Agency, my responsibilities include the investigation of various criminal offenses, including the investigation of financial crimes involving wire fraud and mail fraud.

2. I submit this affidavit in support of an application for a complaint charging ALEXEY SVETLICHNYY with having knowingly and with intent to defraud violated Title 18, United States Code, Sections 1341 and 1343, which prohibit fraudulent schemes that use the mails and interstate or foreign wire communications, respectively.

3. Title 18, United States Code, Section 1341, provides, in pertinent part:

> Whoever, having devised or intended to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, … for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, [commits a crime against the United States].

4. Title 18, United States Code, Section 1343 provides, in pertinent part:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire … communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, [commits a crime against the United States].

5. This affidavit is based on my personal participation in an investigation into

defendant SVETLICHNYY and others and on information provided to me by other law enforcement personnel assisting with the investigation. This affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of a complaint and therefore does not set forth all of the information gathered during this investigation. Statements attributed to individuals are provided in substance and in part.

An Illinois Address Used to Receive Stolen Goods

6. On December 6, 2012, a detective with the Hickory Hills (Illinois) Police Department received a report from ServerSupply, a New York company that sells technology products over the Internet.

7. A ServerSupply employee reported having several days earlier taken an order for an Intel Xeon 8-Core E5-4650 computer processor valued at approximately $3,700 ("the Processor"). ServerSupply shipped the Processor to O.W.,[1] 9447 S. 86th Court, B302, Hickory Hills, Illinois ("the 86th Court Address").

8. The employee also reported that after shipping the Processor, ServerSupply learned from USAA Bank that the USAA-issued credit card number that was used to purchase the Processor was a compromised credit card and that the purchase of the Processor had not been authorized by USAA's actual account holder, O.W.. USAA Bank also told the employee that the primary mailing address on O.W.'s account had only recently been changed to the 86th Court Address (i.e., the same address to which the Employee had shipped the Processor).

9. The Hickory Hills detective interviewed O.W., the USAA Bank account holder. O.W. stated that her true address was in Vestavia, Alabama and that she had not authorized the purchase of the Processor or its shipment to Illinois.

[1] I know O.W.'s true name but have omitted it from this affidavit because there is probable cause to believe that O.W. is a victim of identity theft.

10. On April 5, 2013, law enforcement personnel went to the 86th Court Address and interviewed A.N., a resident there. A.N. stated, in substance and in part, that A.N. had found work with a company called "Hand Express" in the classified section of a Russian language newspaper. A.N. stated that her job was to receive packages at the 86th Court Address and to forward the packages to addresses that Hand Express provided. A.N. stated that she was paid two or three times via Western Union and MoneyGram wire transfers from Russia for re-shipping the packages.

11. A.N. also stated that she sent several of the packages she received to MICAXR, LLC, at the address 268 Main Street, #124, North Reading, Massachusetts 01864-1338.

Defendant SVETLICHNYY Is Associated with MICAXR, LLC

12. The investigation revealed that 268 Main Street in North Reading, Massachusetts housed a UPS Store ("the North Reading UPS Store"), a location where customers can lease a private mail box.

13. On or about July 17, 2013, law enforcement personnel obtained a copy of the "Application for Delivery of Mail Through Agent" for box #124 at the North Reading UPS Store.

14. Review of that application revealed that defendant SVETLICHNYY applied to lease box #124 on July 9, 2012 and provided a driver's license and student identification bearing his photograph. Defendant SVETLICHNYY stated on the application that the business of MICAXR, LLC was "sales".

15. United States Postal Service records indicate that during the two-plus month period between July 25, 2013 and on or about October 10, 2013, box #124 at the North Reading UPS Store received approximately 41 packages from what my investigation has confirmed to be

residential addresses in approximately 30 different states.

MICAXR Sold Hundreds of Items over eBay, Including the Stolen Processor

16. On May 23, 2013, law enforcement personnel obtained records from eBay, the online marketplace, regarding an account in the name of MICAXR, which was registered in eBay's records to defendant SVETLICHNYY at his Tewksbury, Massachusetts residence.

17. eBay's records also revealed that SVETLICHNYY's MICAXR account was used to list for sale and sell hundreds of computer, photographic, and other high-end electronic and technical equipment between in or about March 2010 and in or about February 2014. These items included popular consumer products, such as Apple iPads, Canon cameras and camera lenses, and Samsung cell phones. In total, eBay credited defendant SVETLICHNYY's account with more than $656,000 resulting from the sale of approximately 650 items during that period.

18. These sales included the April 5, 2013 sale of an Intel Xeon E5-4605 processor, the same make and model computer as the Processor purchased without authorization in December 2012 using O.W.'s compromised USAA credit card.

19. eBay's records also revealed the identity of the Chatsworth, California-based customer that purchased the Intel computer processor described in paragraph 18. On December 5, 2013, law enforcement personnel interviewed an employee of that company, who sent a picture of the processor that included its serial number. The provided serial number matched the serial number of the Processor purchased with O.W.'s credit card (and shipped to A.N. at the 86th Court address and later to MICAXR at the North Reading UPS Store).

20. I have reviewed records obtained from Bank of America for a checking and savings account in the name of defendant SVETLICHNYY. Between February 9, 2010 and January 27, 2014, the accounts show electronic deposits from Paypal (which I am aware is an

online payments platform owned by eBay) totaling $427,182.44. There is accordingly probable cause to believe that defendant SVETLICHNYY sold approximately $427,182.44 in merchandise through MICAXR, LLC's eBay account, including the stolen Processor.

Defendant SVETLICHNYY's Suspicious Banking Activity

21. For the period between October 20, 2011 and August 28, 2013, defendant SVETLICHNYY's Bank of America records show twenty wire transfers to a single person, Vyacheslav Tyrapinchkin, totaling $135,401. As set forth in the table below, the wires each went to one of three banks that operate in Russia: Alfa Bank, Unicredit, and Promsvyaz Bank:

Account	Date	Payee Bank	Debit Amount
6885	10/20/2011	Alfa Bank	$1,000.00
7473	10/31/2011	Alfa Bank	$8,000.00
6885	11/7/2011	Alfa Bank	$8,000.00
7473	11/17/2011	Alfa Bank	$9,000.00
6885	12/14/2011	Alfa Bank	$9,000.00
6885	12/20/2011	Alfa Bank	$9,000.00
6885	12/28/2011	Unicredit Bank	$9,000.00
6885	12/28/2011	Unicredit Bank	$1,000.00
6885	12/28/2011	Promsvyaz Bank	$1,000.00
6885	12/29/2011	Promsvyaz Bank	$9,000.00
6885	1/20/2012	Alfa Bank	$9,000.00
7473	3/26/2012	Alfa Bank	$9,000.00
7473	6/11/2012	Alfa Bank	$3,068.00
7473	9/24/2012	Alfa Bank	$9,000.00
7473	2/12/2013	Alfa Bank	$9,000.00
7473	4/9/2013	Alfa Bank	$2,852.00
6885	6/5/2013	Alfa Bank	$981.00
6885	7/17/2013	Alfa Bank	$9,500.00
6885	8/7/2013	Alfa Bank	$9,500.00
6885	8/28/2013	Alfa Bank	$9,500.00

22. As noted in the table above, fourteen of these twenty wire transfers were for between $8,000 and $9,500, amounts just below $10,000. In my training and experience investigating financial crimes, I am aware that individuals often believe that $10,000 is a financial transaction amount at and above which banks are obligated to report wire transfer transactions to U.S. regulatory authorities. Such individuals sometimes structure their wire transfers to avoid the $10,000 threshold, even though that reporting threshold is in actuality applicable only to cash transactions. Defendant SVETLICHNYY's use of repeated sub-$10,000 wire transfers is accordingly an indication of possible fraud.

23. In addition, two sets of wire transfers appear to have been structured to keep wires underneath a $10,000 threshold. Specifically, on December 28, 2011, defendant SVETLICHNYY wired $9,000 to Tryapinchkin at Unicredit Bank and $1,000 to Tryapinchkin at the same bank. Defendant SVETLICHNYY also sent a second $1,000 wire that day to Tryapinchkin at Promsvyaz Bank, for a total of $11,000 wired in three wire transfers to the same recipient on December 28, 2011. The following day, on December 29, 2011, defendant SVETLICHNYY sent another $9,000 to Tryapinchkin's Promsvyaz Bank account. As noted above, SVETLICHNYY's avoidance of the $10,000 "limit" is an indication of fraudulent activity, even if the transactions were not structured cash transactions.

24. In fact, investigators learned that SVETLICHNYY controlled another bank account, Citibank account number 1229129528, to receive payments from Paypal in connection with MICAXR's online sales, until Citibank investigators contacted defendant SVETLICHNYY suspecting fraud.

25. More specifically, between December 28, 2010 and March 30, 2011, eBay/PayPal records indicate that the auction site transferred $96,850 from defendant SVETLICHNYY's

MICAXR account to that Citibank account. In or about late March 2011, however, Citibank investigators noticed the credits from eBay/Paypal, which were unusual for a student account, and that defendant SVETLICHNYY had withdrawn approximately $80,000 in cash, with many of the cash withdrawals in amounts just below $10,000 (i.e., several at $9,500). The investigation to date reveals that Citibank contacted defendant SVETLICHNYY regarding this banking activity.

26. Review of Citibank and eBay records reveals that at or about the time of this contact, defendant SVETLICHNYY stopped using that Citibank account to receive any deposits from eBay/Paypal. Defendant SVETLICHNYY instead transferred MICAXR's eBay proceeds to his Bank of America accounts and sent the sub-$10,000 wires described above.

MICAXR is a Fraudulent Re-Shipping Business

27. Based on my training and experience investigating financial frauds and the investigation to date, defendant SVETLICHNYY's business, MICAXR, bears several indicia of a fraudulent re-shipping scheme.

28. First, based on my training and experience, there is no legitimate reason to have new, high-end electronic and technical equipment purchased, shipped to residential addresses, re-shipped to a business address, and then finally re-sold online and then re-shipped to an end customer, as the Intel Processor described above was in this case. (The data from the U.S. Postal Service in paragraph 15 above similarly indicates that the majority of the parcels shipped to MICAXR at the North Reading UPS Store originated at residential addresses, which is strongly indicative of other parcels that defendant SVETLICHNYY received having been re-shipped. Similarly, as described below, several of the parcels seized from defendant SVETLICHNYY's residence contained invoices showing that those packages had also been shipped to an

intermediary residential address before being forwarded to MICAXR). Paying manufacturer and then re-shippers to ship the same parcels twice inside the United States is irrational. In my experience, the purpose of shipping a product two or more times is to insulate a recipient of stolen goods from an address (such as A.N.'s 86th Court Address) that will inevitably be associated with fraudulent purchases.

29. Second, the use of international wire transfer services to pay re-shippers nominal amounts (as A.N. stated she was paid in paragraph 10 above) strongly suggests fraudulent activity. In my training and experience, I am aware that Western Union charges transaction fees that would make frequent wire transfers an inefficient way to pay employees engaged in a legitimate business.

30. Third, the large number of re-shippers that sent packages to defendant SVETLICHNYY at the North Reading UPS Store (as evidenced by the packages originating from so many different residential addresses) is another inefficiency that a legitimate business that was paying for its inventory would not use. Based on my training and experience investigating similar schemes, the fraud requires a large number of re-shippers because re-shippers like A.N., who are typically the first to receive stolen goods from a retailer, are often the first to be investigated by law enforcement personnel (as A.N. was in this case).

31. In fact, during the course of the investigation, law enforcement personnel learned that SVETLICHNYY opened a second UPS store mailbox in Chelmsford, Massachusetts in August 2013. Records obtained from that Chelmsford UPS store show an additional 55 packages sent to defendant MICAXR and defendant SVETLICHNYY between August 2013 and October 2013 alone. Again, in my training and experience, no legitimate business would pay separately to operate two receiving addresses within miles of each other.

32. Fourth, review of eBay records for SVETLICHNYY's MICAXR account shows that SVETLICHNYY regularly sold equipment at less than the prevailing retail prices for the equipment. For example, the Processor was purchased (with a stolen credit card) for $3,730 from ServerSupply, but defendant SVETLICHNYY's eBay account sold it for only 2,399.95, an approximately 35 percent discount from the purchase price.[2] Defendant SVETLICHNYY could not sustain a business purchasing inventory at full cost and selling it at an approximately 35 percent discount.

33. Fifth, defendant SVETLICHNYY's overseas wire transfers are also indicative of fraud. There is no apparently legitimate reason to split wire transfers to the same named recipient across multiple banks in relatively short time periods. That defendant SVETLICHNYY did this at least twice, and that he consistently kept wires below $10,000, shows that these transactions were purposeful rather than happenstance.

34. Finally, defendant SVETLICHNYY switched his MICAXR activity to Bank of America and limited his overseas wires from Bank of America to amounts below $10,000 after being contacted by Citibank regarding suspicious banking activity. As noted above, shortly after Citibank contacted defendant SVETLICHNYY, he stopped using Citibank to receive MICAXR proceeds and his Bank of America wire transfers were below $10,000. In my training and experience, the change of bank accounts under these circumstances is an indicia of a fraudulent activity.

Defendant SVETLICHNYY Knew That Merchandise Shipped to MICAXR Was Stolen

35. On October 10, 11, and 16, 2013, law enforcement personnel interviewed defendant SVETLICHNYY at his Tewksbury, Massachusetts residence. During these

[2] In fact, the MICAXR eBay account was used to list the Server six separate times beginning an approximately $3,100 and at ever decreasing prices in a span of approximately 70 days.

interviews, defendant SVETLICHNYY stated, in substance and in part, that he was in the business of re-selling high-end electronics on eBay that he received from A.N. and others, and that he wired the proceeds of these sales overseas (less a commission).

36. Defendant SVETLICHNYY also stated that he believed that the all of the electronics he received and re-sold through MICAXR were obtained using stolen payment card information.

37. Law enforcement personnel also took from SVETLICHNYY's Tewksbury residence several packages containing electronic equipment that had been shipped to MICAXR from addresses in New York and Illinois, among other locations. The packages contained, among other things, a laptop computer; a dive watch; a diving computer; several portable water filtration units that typically retail at approximately $400 per unit; and an expensive camera lens.

38. Several of the boxes also contained original invoices from a retailer. Each of the invoices listed one billing address and a second shipping address. The shipping addresses matched the return address on the packages addressed to MICAXR, which is indicative of defendant SVETLICHNYY having received re-shipped (and stolen) consumer goods.

39. One of the packages seized from defendant SVETLICHNYY's residence contained a dive computer that had been shipped to MICAXR at the Chelmsford UPS Store. According to the computer's manufacturer, the product retailed for more than $1,700.

40. Investigators obtained the American Express card number that was used to purchase the dive computer and learned from American Express that its cardholder, S.C., the purported purchaser on the retailer's invoice, had his credit card closed for fraud in or about October 2013, around the time the dive computer arrived at the Chelmsford UPS Store. Interviewed by telephone, S.C. similarly stated he had not authorized the purchase of the dive

computer and another denied charge attempt on his American Express account.

41. Law enforcement personnel also took from SVETLICHNYY's Tewksbury residence approximately 270 gift and prepaid stored value cards valued at $17,850 that SVETLICHNYY stated he had received from others and that he knew to have been purchased using stolen payment card information.

42. Law enforcement personnel obtained records from several of the issuers of these gift cards. Officials from PSE Credit Union, Inc. reported that their accountholder, S.K. of Parma, Ohio, had suffered an approximately $2,500 loss when S.K.'s payment card was used to purchase ten $100 gift cards at Macy's and a single $1,500 gift card from Frontier Airlines. Among the gift cards seized from defendant SVETLICHNYY's residence were ten $100 Macy's gift cards and a $1,500 gift card from Frontier Airlines.

43. Defendant SVETLICHNYY stated he had not sold many of the stored value cards through MICAXR's eBay account because he knew that such cards, when purchased with stolen payment card data, are frequently cancelled when the issuer receives a report that the card was purchased through fraud. Defendant SVETLICHNYY told law enforcement personnel of at least one customer to whom he had to refund money after selling a gift card that turned out to have no value. Defendant SVETLICHNYY told law enforcement personnel that he had stopped selling the gift and stored value cards because a negative user review on eBay (for selling a worthless product) would reduce his ability to distribute other stolen merchandise through the MICAXR account.

CONCLUSION

44. Based on the foregoing, I submit that there is probable cause to believe that between in or about March 2010 and in or about October 2013, defendant ALEXEY

SVETLICHNYY and others did commit mail fraud, in violation of 18 U.S.C. § 1341, and wire fraud, in violation of 18 U.S.C. § 1343.

Respectfully submitted,

KIMBERLY VAGOS BLACKWOOD
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Subscribed and sworn to before me
on May 23, 2014

HONORABLE JUDITH G. DEIN
UNITED STATES MAGISTRATE JUDGE